Christopher J. Schatz, OSB No. 915097
Assistant Federal Public Defender
101 SW Main Street, Suite 1700
Portland, OR 97204
Tel: (503) 326-2123
Fax: (503) 326-5524
Email: chris_schatz@fd.org

Ruben L. Iñiguez
Assistant Federal Public Defender
101 SW Main Street, Suite 1700
Portland, OR 97204
Tel: (503) 326-2123
Fax: (503) 326-5524
Email: ruben_iniguez@fd.org

Attorneys for Hock Chee Khoo

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

PORTLAND DIVISION

UNITED STATES OF AMERICA, **Plaintiff,** **vs.** **HOCK CHEE KHOO, et al.,** **Defendants.**	**CR 09-321-KI** **SUPPLEMENTAL MEMORANDUM OF LAW RE AUTHENTICATION AND DE-FRAGMENTING OF HARD DRIVE.**

Defendant Hock Chee Khoo, through his attorneys of record, Ruben L. Iñiguez and Christopher J. Schatz, hereby supplements his Reply To Government's Response To Motion To Exclude Images Of The Wu Laptop And External Hard Drive [Docket No. 78]. This Supplemental

Memorandum addresses the discovery described by Forensic Computer Expert Michael Bean in his Supplemental Declaration [Docket No. 82], filed on November 12, 2010, at paragraphs 5 and 6:

> 5. In the course of the review described in (4) above, I did make a very unusual discovery. The FTK EnCase image of the Wu Laptop hard drive contains only one file that is recorded as deleted and able to be recovered. This file is named "Ntuser.tmp" and it has a last accessed date of October 21, 2006 (China time), approximately 15 days after the image was purported to have been created by the FBI. This is also inconsistent with the date that the Acronis Backup copy of the Wu hard drive was made, which was October 18, 2006 (China time). This is unusual and surprising in that, during the course of normal computing, files (such as, for example, temporary files) are routinely and automatically deleted without user activity. Consequently, as an experienced forensic computer examiner I expect to find deleted files that are recoverable from unallocated space on the hard drive. The absence of deleted files detectable by forensic software as being recoverable leads me to believe with reasonable forensic certainty that, before the FBI imaged the hard drive, the Wu Laptop hard drive had been altered.
>
> 6. As a result of the unusual and surprising discovery described in (5) above, I conducted an analysis of the unallocated space of the FTK EnCase image of the Wu hard drive made which is where deleted file content resides. The unallocated space contained what appeared to be deleted data in some areas but it also contained large blocks of blank or empty space which is consistent with specific targeted wiping or intentional defragmentation of the hard drive. Defragmentation of a hard drive can easily be accomplished using a utility named "Defrag" which is supplied with the Windows operating system. The file used to execute the "defrag" operation is named "Defrag.exe" and this file is located in the "Windows\System32" directory present in the image made by the FBI of the Wu Laptop hard drive.[1]

A. The Defragmentation Process Prevents Authentication of the Wu Laptop Hard Drive Data Content.

In the course of normal usage, as files are saved, deleted, or moved, files and file parts become fragmented and scattered over various sectors of the computer's hard drive. In addition, when file data saved on contiguous sectors and/or clusters is larger than contiguous free space, the

[1]Further elaboration of his findings will be presented by Mr. Bean at the evidentiary hearing scheduled to take place on November 16, 2010.

computer's operating system will break up the file data and randomly write it to unallocated storage space.[2] The de-fragmenting application ("de-frag") reorganizes files so that they occupy contiguous sector space. Unfortunately, one consequence of employing the de-frag application is that it will over-write information in unallocated space.

Addressing a spoliation issue generated by a defendant's utilization of a defragmentation utility, in *Victor Stanley, Inc. v. Creative Pipe, Inc., et al.*, 2010 WL 3703696 *4 n.14 (D.Md.), the Court stated as follows:

> Disk Defragmenter, Microsoft Window's disk defragmentation program, is a system utility that "consolidates fragmented files and folders on [a] computer's hard disk, so that each occupies a single, contiguous space" in the system. . . . . To consolidate fragmented files, the program moves the file fragments together by "overwriting all those places" where space in the system was occupied by deleted files. As a result, "the ability to recover deleted items virtually ... disappears" because the same is occupied by other files. (Dec. 1, 2009 Hr'g Tr. 43:1-44:18 (Spruill Test.).) **Cutting through all the techno-speak, it is foreseeable that the running of a disk defragmentation program, colloquially referred to as "defragging," can result in the loss of files that were recoverable before the defragmentation occurred.**

(Emphasis added).

An Electronically Stored Information (ESI) file contains both data and metadata. The metadata "describes when a file was created, where it was stored, and what programs the computer uses to help access the file." *Krumwiede v. Brighton Associates*, L.L.C., 2006 WL 1308629 *4 (N.D.Ill.).[3] When an ESI file is moved, read, or deleted, in addition to any changes made to the file's

---

[2]The location of active file data is preserved by the hard drive's File Allocation Table ("FAT") which keeps track of where file data is stored.

[3]As noted by the court in *Pitney Bowes Government Solutions, Inc. v. United States*, 94 Fed.Cl. 1, 8 n.10 (Fed.Cl. 2010):

manifest data, the original file entry's metadata is also modified:

> Any alteration of an original file entry may be significant, however, because the metadata contained in the entry changes, making it impossible to verify that the file is identical to the original, even if the file's content appears unchanged.

Id. When alteration of file data rises to the level of spoliation, as where metadata is lost as a result of file deletion, manipulation, or overwrite, or modification by the running of a de-frag utility, authentication of file data and metadata is rendered impossible:

> As a result of Krumwiede's spoliation of evidence, even if the thousands of altered and modified documents located on Brighton's laptop are not actually deleted, **the changes to the file metadata call the authenticity of the files and their content into question and make it impossible for Brighton to rely on them**. Furthermore, at least 111 files were deliberately deleted and overwritten and are no longer recoverable. It follows that, as a result of Krumwiede's actions, Brighton may no longer rely on evidence essential to its underlying claims and Brighton has been prejudiced by Krumwiede's spoliation of evidence.

Id. at *10 (emphasis added).

Federal Rule of Evidence 901(a) provides that the "requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." Given that (1) the FTK EnCase image of the Acronis backup copy lacks any file-specific metadata, and (2) the FTK EnCase image of the Wu Laptop hard drive contains both manifest and metadata that has been manipulated, deleted, and/or substantially altered in ways that cannot be forensically repaired, as was found to be the case

---

> Microsoft Word files can contain metadata or "data about data" which may indicate "the creation date, the edit date, and the author ..., as well as other descriptive or identifying information" about a particular document. Pl.'s Second Mot. for Judgment at 11; see also id. (citing Black's Law Dictionary 1080 (9th ed.2009), which defines "metadata" as "[s]econdary data that organize, manage, and facilitate the use and understanding of primary data").

in *Krumwiede*, it cannot be determined to any degree of certainty here that the file content preserved in the images is in fact the same file content as was present on the laptop at the time it was seized by Hoffman on October 17, 2006.

B. Preservation of a Defendant's Due Process Right to a Fair Trial in a Criminal Case Requires That the Court Not Admit Evidence That Cannot Be Authenticated.

At a minimum, the defendant in a criminal case has a due process right not to be forced to defend against, and/or to be convicted on the basis of, evidence that has been tainted by manipulation irrespective of whether that manipulation is attributable to the government or merely an unethical and over-zealous third party. *In Re Murchison*, 349 U.S. 133, 136 (1955) ("A fair trial in a fair tribunal is a basic requirement of due process."). The focus of concern presented by Mr. Khoo's authentication objection to the FTK EnCase images of the Wu Laptop computer hard drive and the Acronis backup copy is not the government's failure to preserve evidence (as addressed in *Arizona v. Youngblood*, 488 U.S. 51 (1988)), but the Court's duty to ensure that evidence admitted at the government's request does not bear indicia of manipulation and falsification.

The duty to preserve evidence relevant to litigation is "a duty owed to the *court*, not to a party's adversary." *Creative Pipe*, 2010 WL 3703696 *26. Where the matters at issue involve computer data, the "general duty to preserve may also include deleted data, data in slack spaces, backup tapes, legacy systems, and meta data . . .." Paul W. Grimm, *Proportionality In The Post-Hoc Analysis Of Pre-Litigation Preservation Decisions*, 37 U. Batl. L. Rev. 382, 410 (2008). Spoliation of evidence occurs where evidence having a reasonably foreseeable value to contemplated or existing litigation is destroyed or altered. *West v. Goodyear Tire & Rubber Co.*, 167 F.3d 776, 779 (2d Cir. 1999). The courts possess inherent authority to impose sanctions for spoliation of evidence as a

means of preserving "the integrity of the judicial process" so that litigants do not lose "confidence that the process works to uncover the truth." *Silvestri v. General Motor Corps.*, 271 F.3d 583, 590 (1st Cir. 2001).[4]

C. Conclusion.

In light of the above, and given the findings made by Forensic Computer Expert Michael Bean, neither of the FBI's FTK EnCase images can be adequately authenticated per the terms of Federal Rule of Evidence 901(a). Nor can any printout of a document or file content be admitted as a duplicate of the data contained in either image insofar as a "genuine question" has been raised as to the "authenticity of the original" images. *See* Federal Rule of Evidence 1003(1).

Respectfully submitted this November 15, 2010.

/s/ Christopher J. Schatz
Christopher J. Schatz
Assistant Federal Public Defender

Attorney for Defendant Khoo

[4]The court's inherent authority arises "when a party deceives a court or abuses the process at a level that is utterly inconsistent with the orderly administration of justice or undermines the integrity of the process." *United States v. Shaffer Equip. Co*., 11 F.3d 450, 462 (4th Cir. 1993).